**PCT** WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

| (51) International Patent Classification 6 : H04L 29/06 | A1 | (11) International Publication Number: WO 99/38302 |
|---|---|---|
| | | (43) International Publication Date: 29 July 1999 (29.07.99) |

(21) International Application Number: PCT/GB98/00185

(22) International Filing Date: 22 January 1998 (22.01.98)

(71) Applicant *(for all designated States except US)*: MAXON SYSTEMS INC. (LONDON) LTD. [GB/GB]; Maxon House, Honeycrock Lane, Salfords, Surrey RH1 5JP (GB).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: YUN, Du, Yung [US/KR]; 1053, Namhyun-dong, Kwanak-ku, Seoul (KR). PATEL, Chris [GB/GB]; 35 Sandcroft Road, Charlton, London SE7 7LR (GB).

(74) Agent: SCHMIDT, Steffen, J.; Wuesthoff & Wuesthoff, Patent- und Rechtsanwälte, Schweigerstrasse 2, D-81541 München (DE).

(81) Designated States: KR, US, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
*With international search report.*

(54) Title: SECURE DATA COMMUNICATION SYSTEM

(57) Abstract

A secure data communication system comprising a first computer (10, 16) is adapted to transmit/receive information to/from a second computer (12) via a first communication path (14). The first computer (10, 16) is adapted to transmit/receive information to/from a second computer (12) via a second communication path (20) distinct from the first communication path (14), and the first computer (10, 16) is adapted to split the information into at least two different portions of partial information prior to transmitting the information to the second computer, and transmit the at least two different portions of partial information via the first and the second communication path. The second computer (12) is adapted to receive at least two different portions of partial information from the first computer via the first and the second communication path, and combine the at least two different portions of partial information to obtain the original information.

*FOR THE PURPOSES OF INFORMATION ONLY*

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **AL** | Albania | **ES** | Spain | **LS** | Lesotho | **SI** | Slovenia |
| **AM** | Armenia | **FI** | Finland | **LT** | Lithuania | **SK** | Slovakia |
| **AT** | Austria | **FR** | France | **LU** | Luxembourg | **SN** | Senegal |
| **AU** | Australia | **GA** | Gabon | **LV** | Latvia | **SZ** | Swaziland |
| **AZ** | Azerbaijan | **GB** | United Kingdom | **MC** | Monaco | **TD** | Chad |
| **BA** | Bosnia and Herzegovina | **GE** | Georgia | **MD** | Republic of Moldova | **TG** | Togo |
| **BB** | Barbados | **GH** | Ghana | **MG** | Madagascar | **TJ** | Tajikistan |
| **BE** | Belgium | **GN** | Guinea | **MK** | The former Yugoslav Republic of Macedonia | **TM** | Turkmenistan |
| **BF** | Burkina Faso | **GR** | Greece | | | **TR** | Turkey |
| **BG** | Bulgaria | **HU** | Hungary | **ML** | Mali | **TT** | Trinidad and Tobago |
| **BJ** | Benin | **IE** | Ireland | **MN** | Mongolia | **UA** | Ukraine |
| **BR** | Brazil | **IL** | Israel | **MR** | Mauritania | **UG** | Uganda |
| **BY** | Belarus | **IS** | Iceland | **MW** | Malawi | **US** | United States of America |
| **CA** | Canada | **IT** | Italy | **MX** | Mexico | **UZ** | Uzbekistan |
| **CF** | Central African Republic | **JP** | Japan | **NE** | Niger | **VN** | Viet Nam |
| **CG** | Congo | **KE** | Kenya | **NL** | Netherlands | **YU** | Yugoslavia |
| **CH** | Switzerland | **KG** | Kyrgyzstan | **NO** | Norway | **ZW** | Zimbabwe |
| **CI** | Côte d'Ivoire | **KP** | Democratic People's Republic of Korea | **NZ** | New Zealand | | |
| **CM** | Cameroon | | | **PL** | Poland | | |
| **CN** | China | **KR** | Republic of Korea | **PT** | Portugal | | |
| **CU** | Cuba | **KZ** | Kazakstan | **RO** | Romania | | |
| **CZ** | Czech Republic | **LC** | Saint Lucia | **RU** | Russian Federation | | |
| **DE** | Germany | **LI** | Liechtenstein | **SD** | Sudan | | |
| **DK** | Denmark | **LK** | Sri Lanka | **SE** | Sweden | | |
| **EE** | Estonia | **LR** | Liberia | **SG** | Singapore | | |

SECURE DATA COMMUNICATION SYSTEM

The present invention is related to a secure data communication system. More specifically, the present invention is related to a secure data communication system in which an end user is capable of interchanging data with a host computer.

Today, an increasing number of transactions are carried out between end users (e.g. at home) and host computers (e.g. of a bank). These transactions can include money orders occuring when an end user does "electronic shopping" (e.g. home order television) or the transmission of other sensitive data.

In current systems, protection schemes include the encryption of the data by various algorithms (e.g. DES or RSA). However, the transmission of information encripted according to such algorithms is not immune to wire tapping and subsequent decryption. The likelihood of a successful decryption is increased by the increased computational power of computer work stations available today.

Hence, it is an object of the present invention, to provide a simple but secure data communication system which can be implemented for a virtually unlimited number of end users who want to communicate with a host computer.

To solve this problem, the present invention teaches a secure data communication system comprising a first computer being adapted to transmit/receive information to/from a second computer via a first communication path, wherein the first computer is adapted to transmit/receive information to/from a second computer via a second communication path distinct from the first communication path, the first computer is adapted

to split the information into at least two different portions of partial information prior to transmitting the information to the second computer, transmit the at least two different portions of partial information via the first and the second communication paths, respectively, the second computer being adapted to receive at least two different portions of partial information from the first computer via said first and said second communication path, and combine the at least two different portions of partial information to obtain the original information.

This concept makes it very difficult if not impossible for any intruder to obtain the complete information sent/received. Since the splitting of the information into various portions can be done in a manner unpredictable by an intruder, he/she will not be able to obtain the complete information by only tapping on of said communication paths.

Moreover, even if the intruder were able to tap both or all of said communication paths, there remains still the difficulty for him/her to (re)combine the obtained respective portions of the information in a useful manner.

Preferably, the first and the second computer further comprise an information splitting/combination means to split information to be sent and/or to store received different portions of partial information and to combine said received and stored different portions of partial information to obtain the original information.

This can either be implemented in the respective computers themselves by software programs, or the first and the second computer are connected to external hardware devices, respectively, in which these function are implemented (by a suitably programmed computer).

The information splitting/combination means also includes a determination means (preferably implemented by a software program) to determine an splitting scheme according to which the different portions of partial information from the first computer are splitted and sent via said first and said second communication path to said second computer.

This allows for a pseudo-random splitting of the transmission of the different portions of partial information from the first computer to the second computer (and vice versa) via the two communication paths. This scheme makes it virtually unpredictable for an intruder to obtain the complete information in a legible manner.

To make it even more difficult, it is also possible to additionally reverse or at least change the sequence of the different portions of partial information in each of the two communication paths.

The determination means is adapted to determine the order of splitting according to a predetermined scheme or a random scheme. A predetermined order scheme is easier to implement (on the transmitting side as well as on the receiving side) but also easier to be found out by an intruder.

A random order scheme requires a more sophisticated mechanism or protocol to ascertain the correct concatenation of the different portions of partial information at the receiving side of the communication path.

The invention is also covering the concept of transceiving information that is accompanied by a PIN (Personal Identification Number) and/or a TAN (Transaction Number). According to the invention, the PIN and/or the TAN as well as the information itself can be split according to various schemes. One example is to sent any or all Arabic numerals through one communication path, while the remaining

information is sent through the other communication path. Preferably, in the case of the two communication paths having different levels of security, the Arabic numerals would be sent through communication path having the higher security level.

Another possibility is to change the communication path after each Arabic numeral character sent. Thus, especially the highly sensitive parts of the information are broken into entities which are meaningless (and hence worthless) to any intruder.

In a preferred embodiment of the invention, the first communication path is provided in a terrestrial telephone system, and the second communication path is provided in a cellular mobile telephone system. Especially the usage of the widely spread GSM (R), PCS, CDMA etc. systems with their superior level of safety compared to land lines makes it extremely difficult for an intruder to obtain the complete information transceived (irrespective of whether or not the information is transmitted in an encrypted format or not).

The present invention also encompasses that the first and/or said second computer further comprises an information encrypting/decrypting means in which said information is encrypted prior to being split into said at least two different portions of partial information or said information is encrypted after being split into said at least two different portions of partial information. Again, this can be implemented either in the respective computers themselves by software programs, or the first and the second computer are connected to external hardware devices in which these function are implemented (by a suitably programmed computer).

Encrypting the data before the splitting can be advantageous insofar, as the computational power for the encryption algorithm needs to be provided only once while the

computational power to split (and subsequently transmit) the information is relatively limited. It can, however, further increase the security to split the information and to independently encrypt the two parts of the information to be transmitted.

In case the "natural" sequence of the parts of information is changed for one or all of the communication paths, it is preferred to provide an information tagging means in which the at least two different portions of partial information are provided with markings containing an indication regarding the sequential order of the different portions of partial information.

In a preferred embodiment of the invention, the first and the second computer further comprises an information processing means in which information received from a respective other computer is only processed upon an authorization indication generated by a authorization computer connected to the information processing means.

Usually, this authorization computer is provided at the host computer (i.e. the processing computer) of a bank or the like. This processing computer of the bank will obtain the authorization from the authorization computer which is not accessible from outside. Since the processing computer of the bank is only provided with parts of the information required to carry out a certain transaction while the authorization computer is not accessible from outside but only accessible from the processing computer, an intruder will not be able to obtain the complete information.

The present invention is also related to a peripheral device connectable to a computer, said peripheral device comprising: a first input/output connector for transceiving information to/from said computer from/to said peripheral device, a second input/output connector for transceiving information

to/from said peripheral device from/to a first interface connectable to a first communication path, a third input/output connector for transceiving information to/from said peripheral device from/to a second interface connectable to a second communication path, and a controller for controlling the transmission/reception of information to/from said computer from/to said peripheral device, processsing said information and transceiving said information to/from said peripheral device from/to said first and/or second interface from/to said first and/or second communication path. This device can be easily connected to a PC or an intelligent telephone on the one side and to a terrestrial telephone line and a mobile telephone (or a second terrestrial telephone line) in order to set up two communication paths to a host computer (of a bank etc.) Alternatively, it is also possible to use two mobile telephones to set up the two communication paths.

Further features, advantages, possible modifications and enhancements of the present invention are explained in more detail in connection with the description of a presently preferred embodiment as schematically shown in the drawings.

Fig. 1 schematically shows a block diagram of the system according to the present invention.

Fig. 2 schematically shows a block diagram of a peripheral device connectable to a computer to implement the present invention.

Fig. 3 is a schematical flow chart for the program of the computer in the peripheral device according to Fig. 2.

Fig. 4 shows how information presented to the peripheral device according to Fig. 2 is transformed by this device.

In Fig. 1, a secure data communication system is shown. This system comprises a first computer 10 being adapted to transmit/receive information to/from a second computer 12 via a first communication path 14. This first computer can be implemented by a PC (personal computer) having a central processing unit including RAM, ROM, hard disk drive, serial interface etc., a keyboard and a video screen. Alteratively, this computer can also be implemented by a "intelligent" telephone 16 having the standard functions of a telephone plus the capability of entering and displaying one or more lines of alphanumerical characters that are to be transceived by the "intelligent" telephone.

One commercially available product fulfilling these criteria is the telecommunications enduser device "MULTIKIT" marketed by the applicant/assignee of the present invention. This computer/telephone 10, 16 is connected to a peripheral device 22. The peripheral device 22 provides (via a modem or the like) a connection to first communication path 14. This first communication path 14 is a terrestrial telephone network.

Additionally, the first computer 10, 16 is adapted to transmit/receive information to/from the second computer 12 via a second communication path 20 which is different from the first communication path 14. To achieve this, the peripheral device 22 is adapted to split the information received from the first computer 10, 16 into two or more different portions of partial information prior to transmitting the information to the second computer 12. These portions of partial information are transmitted separately via the first and the second communication paths 14, 20. Correspondingly, the second computer 12 is adapted to receive these two different portions of partial information from the first computer 10, 16 via the first and the second communication paths 14, 20, and to combine the two different

portions of partial information to obtain the original (complete) information for further processing.

More specifically, the first computer 10, 16 is connected to a serial interface 28 of the peripheral device 22 which also includes an information splitting/combination functionality to store the information for further processing, i.e. to split information to be sent into different portions of partial information and to combine received different portions of partial information to obtain the original information.

To achieve this, the information splitting/combination device 22 comprises a microprocessor 30 (see Fig. 2), a RAM memory 32 connected thereto, two serial interfaces 34, 36 to provide connections to the mobile telecommunications network 20 and the terrestrial (fixed) network 14, respectively, and a (Flash-)ROM memory 38 for a control software program.

The microprocessor 30 is also programmed to act as a determination means for determining an splitting scheme according to which the different portions of partial information from the first computer 10, 16 are splitted and sent via the first and second communication paths 14, 20 to the second computer 12.

In the present embodiment, the entire information is splitted into different portions of partial information by changing the communication path through which the information is sent after each second character.

More specifically, the splitted portions of information are sent out in an alternating fashion through the two serial interfaces 34, 36 to the mobile telephone 18 having a data transmission/reception capability, and the terrestial telephone network 14, respectively. The portion of the information sent out through the mobile telephone 18 is fed

into the mobile telephone network 20. From the mobile telephone network 20, the portion of the information is sent to a transceiving station 40 provided at the site of the second computer 12. The information received from the mobile network 20 is temporarily stored in an authorization server 44.

Parallel to the transmission of information through the wireless (mobile) communications path 20, the peripheral device 22 feeds ther other portion of information into the terrestrial telephone network 14. The terrestrial telephone network 14 feeds the information into a transceiving station 42 also provided at the site of the second computer 12. The information received by the transceiving station 42 is fed into the second (main) computer 12. Once the second computer 12 receives information through the terrestrial network 14, the corresponding (still missing) information received via the mobile network 20 is obtained by the second computer 12 from the authorization server 44 in order to have the authorization server 44 to carry out the respective transaction.

The second computer 12 (and/or the authorization server 44) are programmed to carry out the decryption and recombination required to reverse the transformation of the information carried out in the first computer/telephone 10/16 or the peripheral device 22.

The microprocessor 30 in the peripheral device 22 is also programmed to act as a an information encrypting/decrypting means in which the information is encrypted prior to being split into the at two different portions of partial information.

Although the separation of the information into two different channels already provides a significant enhancement over current procedures, an intruder actually capable of tapping a

both the terrestrial and the mobile telephone lines could obtain the complete information. Also, an intruder capable of monitoring only one of the two telephone lines (preferably the terrestrial telephone line), could find out at least a part of the sensitive information (e.g. the PIN of a user) by monitoring and analyzing a sufficient number of information transactions. Hence, an additional encryption is desirable. To achieve this, the information can also be encrypted after being split into the two different portions of partial information.

Moreover, the microprocessor 30 is also programmed to act as an information tagging means in which said at least two different portions (AB, CD, EF, GH, IJ, KL) of partial information are provided with markings (1, 2, 3, 4, 5, 6) containing an indication regarding the sequential order of the different portions of partial information. This indication is also be encrypted together with the information portions in order to avoid an intruder being able to immediately gather the order of the information transmitted via one or both communication paths.

The microprocessor 30 can carry out a program according to the flow chart of Fig. 3. The corresponding transformation of the data structure is shown in Fig. 4.

It is understood that the flow of information from the second computer to the first can be carried out in a way corresponding to the procedure described above.

Claims

1. A secure data communication system comprising
- a first computer (10, 16) being adapted to transmit/receive information to/from a second computer (12) via a first communication path (14), characterized in that
- said first computer (10, 16) being adapted to transmit/receive information to/from a second computer (12) via a second communication path (20) distinct from said first communication path (14),
- said first computer (10, 16) being adapted to
-- split the information into at least two different portions of partial information prior to transmitting the information to the second computer,
-- transmit the at least two different portions of partial information via said first and said second communication path,
- said second computer (12) being adapted to
-- receive at least two different portions of partial information from the first computer via said first and said second communication path, and
-- combine said at least two different portions of partial information to obtain the original information.

2. The secure data communication system of claim 1, wherein said first and/or said second computer further comprises
- an information splitting/combination means to split information to be sent and/or to store received different portions of partial information and to combine said received and stored different portions of partial information to obtain the original information.

3. The secure data communication system of claim 1 or 2, wherein each information splitting/combination means comprises
- a determination means to determine an splitting scheme according to which the different portions of partial

information from the first computer are splitted and sent via said first and said second communication path to said second computer.

4. The secure data communication system of claim 3, wherein
- the determination means is adapted to determine the order of splitting according to a predetermined scheme or a random scheme.

5. The secure data communication system of claim 1, 2, or 3, wherein
- the first communication path is provided in a terrestrial telephone network, and
- the second communication path is provided in a cellular mobile telephone network.

6. The secure data communication system of any of claims 1 to 5, wherein the first and/or said second computer further comprises
- an information encrypting/decrypting means in which
-- said information is encrypted prior to being split into said at least two different portions of partial information or
-- said information is encrypted after being split into said at least two different portions of partial information.

7. The secure data communication system of any of claims 1 to 6, wherein the first and/or said second computer further comprises
- an information tagging means in which said at least two different portions of partial information are provided with markings containing an indication regarding the sequential order of the different portions of partial information.

8. The secure data communication system of any of claims 1 to 7, wherein the first and/or said second computer further comprises

- an information processing means in which information received from a respective other computer is only processed upon an authorization indication generated by a authorization computer connected to the information processing means.

9. A peripheral device connectable to a computer, said peripheral device comprising:
- a first input/output connector for transceiving information to/from said computer from/to said peripheral device,
- a second input/output connector for transceiving information to/from said peripheral device from/to a first interface connectable to a first communication path,
- a third input/output connector for transceiving information to/from said peripheral device from/to a second interface connectable to a second communication path, and
- a controller for controlling the transmission/reception of information to/from said computer from/to said peripheral device, processsing said information and transceiving said information to/from said peripheral device from/to said first and/or second interface from/to said first and/or second communication path.

Fig. 1

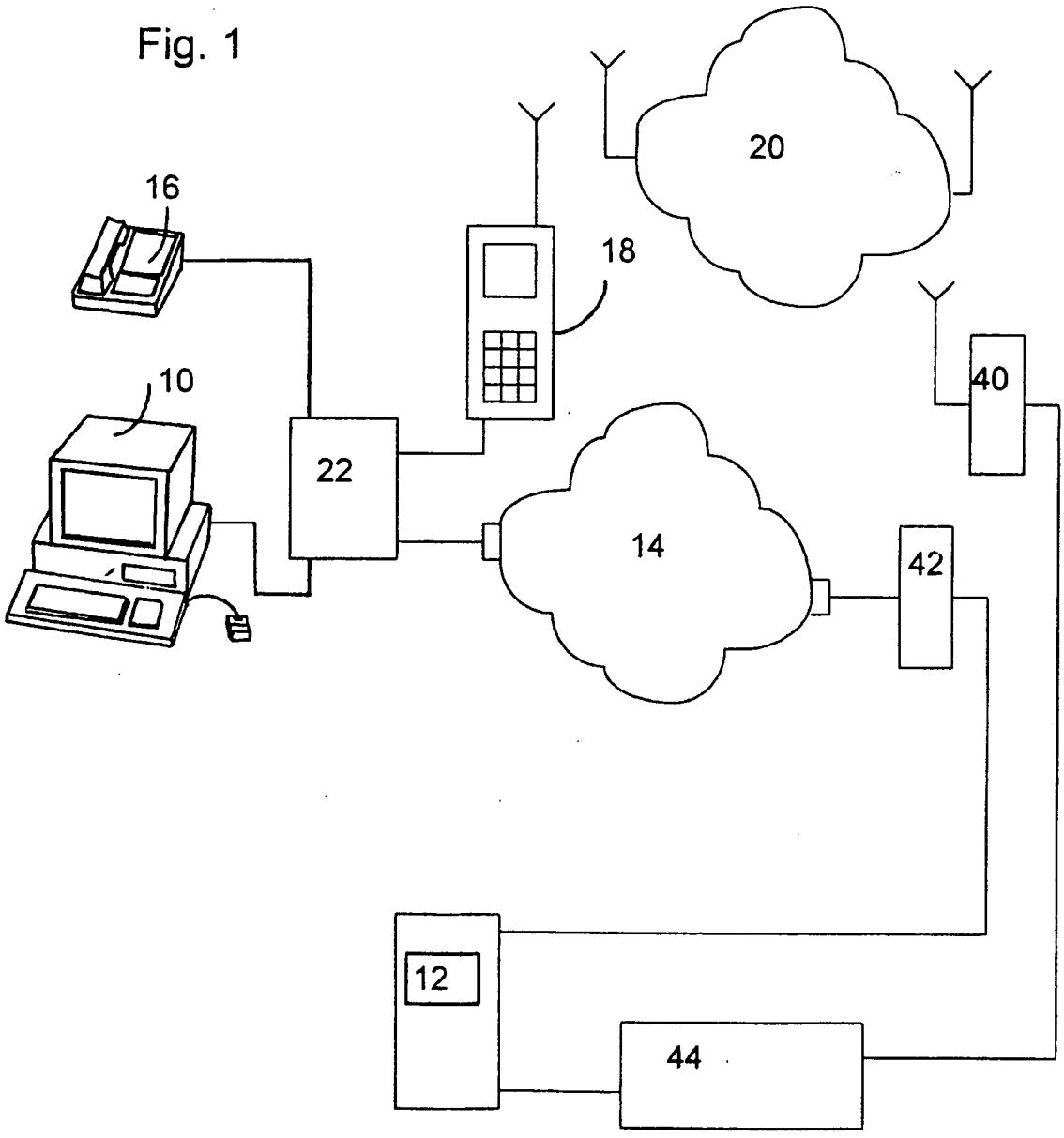


Fig. 2

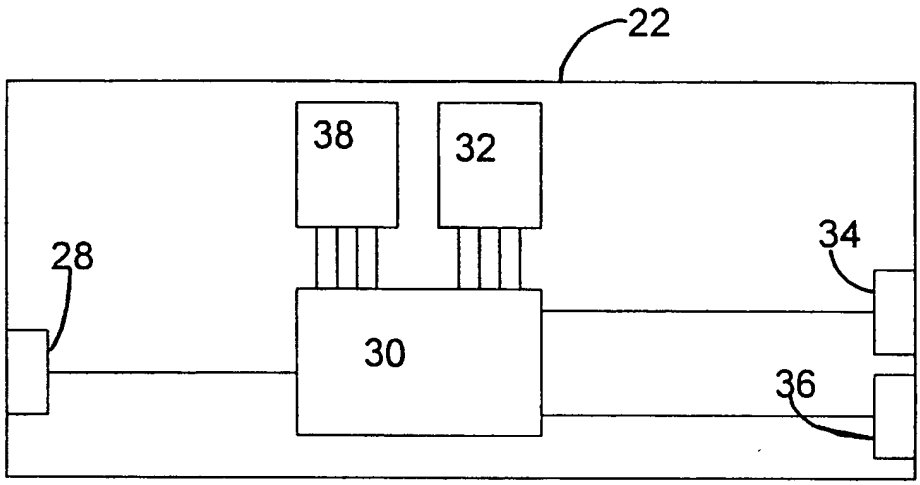
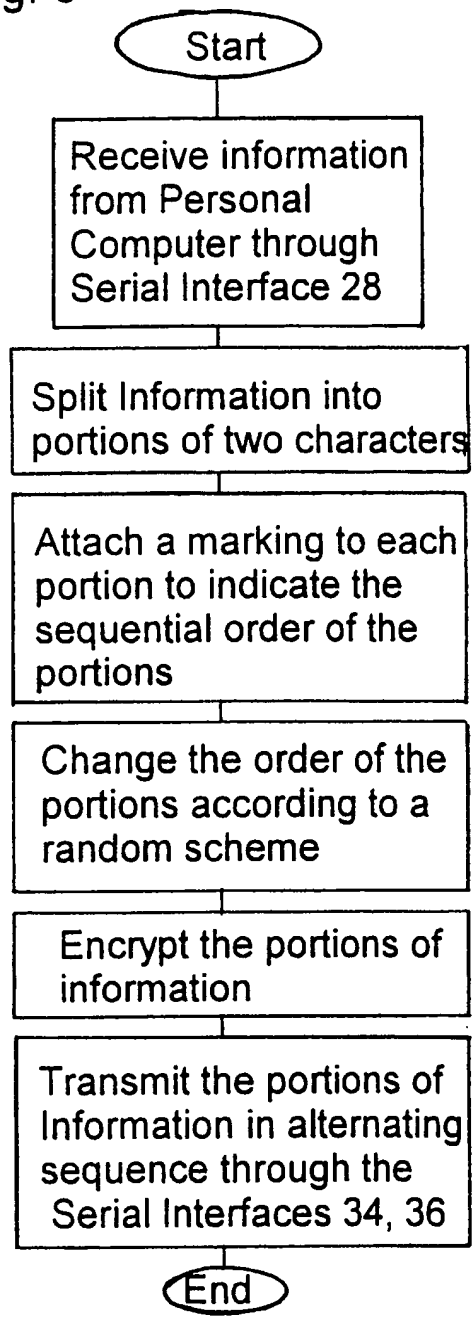


Fig. 3


Start
Receive information from Personal Computer through Serial Interface 28
Split Information into portions of two characters
Attach a marking to each portion to indicate the sequential order of the portions
Change the order of the portions according to a random scheme
Encrypt the portions of information
Transmit the portions of Information in alternating sequence through the Serial Interfaces 34, 36
End

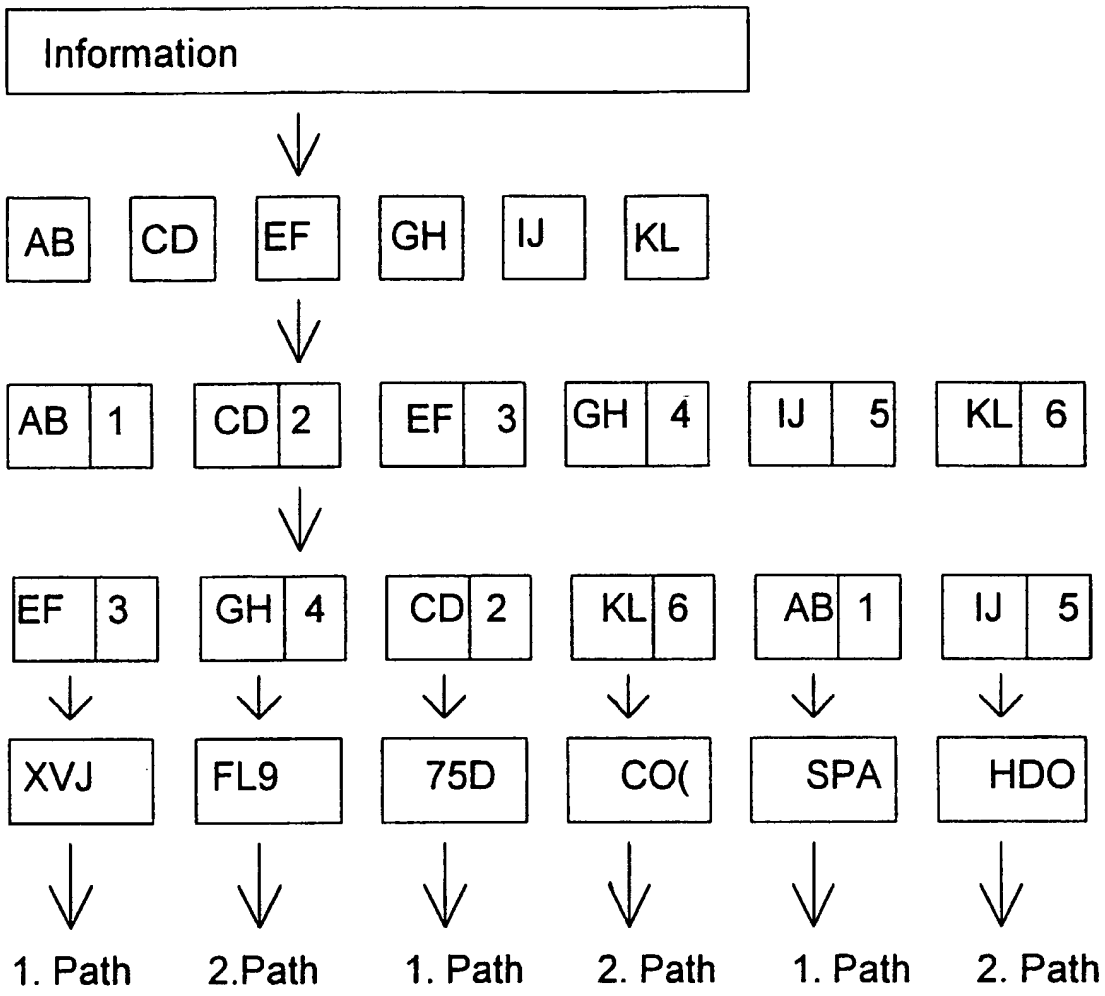

Information
AB
CD
EF
GH
IJ
KL
AB 1
CD 2
EF 3
GH 4
IJ 5
KL 6
EF 3
GH 4
CD 2
KL 6
AB 1
IJ 5
XVJ
FL9
75D
CO(
SPA
HDO
1. Path
2.Path
1. Path
2. Path
1. Path
2. Path

Fig.4

# INTERNATIONAL SEARCH REPORT

Interr ıal Application No
PCT/GB 98/00185

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L29/06

According to International Patent Classification(IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category ° | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | EP 0 224 895 A (AMERICAN TELEPHONE & TELEGRAPH) 10 June 1987<br>see abstract | 1-3,7 |
| Y | see page 3, line 13 - page 7, line 23 | 4,5 |
| Y | EP 0 405 989 A (INMOS LTD) 2 January 1991<br>see page 3, line 15 - line 32<br>see page 16, line 19 - line 43<br>see abstract | 4 |
| Y | US 5 428 671 A (DYKES DON A ET AL)<br>27 June 1995<br>see abstract<br>see figure 1<br>see claim 1 | 5 |

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 20 November 1998 | 26/11/1998 |

| Name and mailing address of the ISA | Authorized officer |
|---|---|
| European Patent Office, P.B. 5818 Patentlaan 2<br>NL - 2280 HV Rijswijk<br>Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,<br>Fax: (+31-70) 340-3016 | Canosa Areste, C |

2

Form PCT/ISA/210 (second sheet) (July 1992)

# INTERNATIONAL SEARCH REPORT

Interr ıal Application No
PCT/GB 98/00185

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

| Category ° | Citation of document, with indication,where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | EP 0 814 589 A (AT & T CORP)<br>29 December 1997<br>see abstract<br>see page 2, line 46 - page 3, line 2<br>see page 3, line 54 - page 4, line 29<br>see figure 3 | 9 |
| A | --- | 1-8 |
| X | WO 95 23471 A (NOKIA TELECOMMUNICATIONS OY<br>;ALMAY HEIKKI (FI)) 31 August 1995<br>see the whole document | 1-4 |
| | ----- | |

2

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

# INTERNATIONAL SEARCH REPORT

...ormation on patent family members

Intern al Application No
PCT/GB 98/00185

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| EP 0224895 A | 10-06-1987 | US 4703475 A | 27-10-1987 |
| | | CA 1264365 A | 09-01-1990 |
| | | JP 62277829 A | 02-12-1987 |
| EP 0405989 A | 02-01-1991 | DE 69029763 D | 06-03-1997 |
| | | JP 3132130 A | 05-06-1991 |
| | | US 5422879 A | 06-06-1995 |
| | | US 5422881 A | 06-06-1995 |
| | | US 5130977 A | 14-07-1992 |
| | | US 5327127 A | 05-07-1994 |
| US 5428671 A | 27-06-1995 | AU 5667994 A | 08-06-1994 |
| | | CA 2147120 A | 26-05-1994 |
| | | EP 0679322 A | 02-11-1995 |
| | | JP 7508870 T | 28-09-1995 |
| | | WO 9411999 A | 26-05-1994 |
| | | US 5408520 A | 18-04-1995 |
| | | US 5737397 A | 07-04-1998 |
| EP 0814589 A | 29-12-1997 | CA 2204058 A | 19-12-1997 |
| WO 9523471 A | 31-08-1995 | FI 940940 A | 29-08-1995 |
| | | AU 681946 B | 11-09-1997 |
| | | AU 1813695 A | 11-09-1995 |
| | | CN 1142298 A | 05-02-1997 |
| | | EP 0749652 A | 27-12-1996 |
| | | JP 10503332 T | 24-03-1998 |